

各位網路先進台鑒：

我們係由政府機關所組成之國際團體，在此謹代表相關政府商請 貴公司參與全球反制垃圾郵件活動，防止垃圾郵件散播者入侵消費者電腦濫發垃圾郵件，使之淪為「Spam 僵屍電腦(Spam Zombies)」。而我等政府機關所要做的即透過法律執行、技術研發、消費者及企業教育、政策制定、以及公私部門合作，來打擊非法垃圾郵件。

垃圾郵件散播者使用家用電腦來散播數以百萬計之大量郵件，他們利用這些電腦的安全漏洞安裝隱藏程式，以之作為郵件伺服器或代理伺服器。他們透過這些「Spam 僵屍電腦」散播大量郵件，藉以隱藏其真實出處。

目前電子郵件體系之完整正遭受僵屍電腦散佈垃圾郵件之威脅，而 貴公司身為網際網路服務提供者(ISP)，自然利害與共。此外，收件人也可能因為垃圾郵件係由 貴公司之系統或 貴公司之顧客系統轉來而責怪 貴公司。同時對 貴公司的網路連接也造成不必要的負擔，增加行政成本。

倘若 貴公司尚未做好相關防護措施¹，建議您可採以下自願性反制僵屍電腦措施：

- 除了經客戶郵件伺服器認證之用戶所作之SMTP發送要求外，請封鎖 port 25。對於那些必須使用外發郵件伺服器之用戶，則建議利用port 587執行具認證功能之SMTP。
- 採用郵件延遲之速限管制。
- 找出電子郵件發送數量異常之電腦，並依步驟檢視判斷該電腦是否為Spam僵屍電腦。必要時，隔離中毒電腦直到移除問題來源。
- 給予顧客簡單易懂的建議，教他們如何防止電腦遭病毒、特洛伊程式或其他惡意軟體感染而成為Spam僵屍電腦，同時提供適當之工具及協助。
- 如果顧客之電腦已中毒，則提供或告知顧客容易使用之工具以移除僵屍碼，並提供必要之協助。

最後，除鼓勵網際網路服務提供者防止垃圾郵件僵屍電腦之形成外，我們正積極從事一項計畫，企圖找出全球可能的僵屍電腦 IP位址，以及所屬之網際網路服務提供者和其他連網服務提供者。該項分析將根據垃圾郵件資料庫及WHOIS資料庫等公開資訊為之。我們計劃聯絡僵屍電腦所在IP位址之網際網路連網服務提供者，並發出第2封信要求該等業者加強解決其系統有關垃圾郵件僵屍電腦之問題。

欲查詢本計畫相關資訊以及參與機關清單，請參閱：

<http://www.ftc.gov/bcp/online/edcams/spam/zombie/index.htm>。

感謝您對於打擊垃圾郵件所給予之協助。

- 1 如果 貴公司採行這些建議，請確認這些措施並未違反 貴國任何現行法律，如資料保護法、隱私或資訊安全法、或其他法制規定或義務，並注意在某些國家司法管轄權下這些建議可能已屬強制規定。